BaanERP 5.0c Tools

User Management

Module Procedure UP093A US

Document information

Document

Document code	: UP093A US
Document group	: User Documentation
Document title	: User Management
Application/Package	: BaanERP 5.0c Tools
Edition	: A
Date	: December 1999

Table of contents

About this document

Read this document to get an overview of the User Management module's functionality and to learn more about the functional procedures that are related to user management.

You need no detailed knowledge of the BaanERP software to read this document. However, you are more likely to understand the contents if you are familiar with the overall structure of packages, modules, and sessions within the BaanERP software.

For detailed descriptions of the module's sessions, refer to BaanERP's comprehensive online Help.

To use this document

Read Chapter 1, The User Management module in BaanERP, if you want to know more about:

- The module's functionality
- The relationship of the module with other modules
- The functionality of the module's business objects

Read Chapter 2, Creating BaanERP users, if you want to know more about:

- How to create BaanERP users
- The results of the procedure
- The sessions in the procedure
- How to define additional user settings
- How to define default user settings

Read Chapter 3, Defining the normal user's authorizations with the Authorization Management System (AMS) business object, if you want to know more about:

- How to define the user's roles and subroles
- How to define the authorizations by role for a normal user
- How to convert the roles and authorizations to the run-time data dictionary

Read Chapter 4, Using templates in the Authorization Management System (AMS) business object, if you want to know more about:

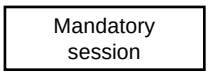
- How to define templates that contain relevant data for a group of users
- How to convert the templates to the run time data dictionary
- How to connect the BaanERP user to a template

Read Chapter 5, Using the role browser, if you want to know how you can use a graphical user interface to view the user's roles.

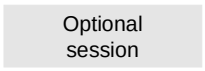
Acronyms and definitions used in this document

AMS	Authorization Management System
Authorizations	A set of permissions that limit the access to various objects in BaanERP. For example, sessions, tables, and companies.
COM	Component Object Model. A specification developed by Microsoft for building software components that can be assembled into programs or add functionality to existing programs that run on Microsoft Windows platforms.
DBA	Database Administrator
DDE	Dynamic Data Exchange. A communication method which allows two or more programs that are running simultaneously to exchange data and commands.
DLL	Dynamically Linked Library. A means of sharing functions between several programs that are running at the same time. This library contains functions for common use. The library can be linked to the object at function call, and at run-time. Implementation of a DLL reduces the size of objects to a minimum because the standard program is no longer merged with each program script.
OCX	Short for OLE custom control. A software module that is based on OLE and COM technologies and that, when called by an application, produces a control that adds some desired feature to the application.
OLE	Object Linking and Embedding. A technology for transferring and sharing information among applications.
ORB	Object Request Broker. In client/server applications, an interface to which the client makes a request for an object. The ORB directs the request to the server that contains the object and then returns the resulting values to the client.
Role	From a users point of view, a function, or part of a function in an organization. For example, manager, secretary, and so on. From an authorization point of view, an identifying name for a group of users. A role can contain several subroles.
Template	A predesigned document that is used to maintain common data for a group of users with the same role.
VRC	Version Release Customization

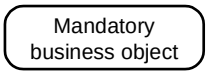
Legend



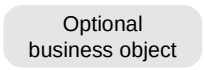
Indicates a mandatory session



Indicates an optional session



Indicates a mandatory business object



Indicates an optional business object

Indicates a package

Indicates a module

Indicates a module that is described in the module procedure

1. The User Management module in BaanERP

This chapter provides information about:

- User management as applied in BaanERP
- User management's functional procedures
- The modules related to user management

1.1 User Management as applied in BaanERP

The User Management module is part of Baan Tools. You can use it to enter user data into the system to enable the users to work with the BaanERP software. This means that the BaanERP users must have a user logon and a password.

Note

For the description of the User Management module it is assumed that the user has a system logon for the operating system. For more information on how to create the user account on the operating system, refer to the appropriate installation manual.

1.2 User Management's functional procedures

The User Management module contains the following functional procedures, which you can use to create a BaanERP user with the proper authorizations:

- Creating BaanERP users
- Defining the BaanERP user's authorizations

The User Management module contains the following business objects:

- General User Data
- Authorization Management System
- Text Parameters
- Developers Data
- Miscellaneous

General User Data

You can use the General User Data business object to enter the basic user data required to create a BaanERP user. For example, user type, BaanERP logon, language code, and so on.

General User Data also provides the tools needed to create remote user accounts for the BaanERP user on remote or distributed databases, and split user interfaces.

Authorization Management System (AMS)

To be able to use BaanERP, a user must have some authorizations. You can use the AMS business object to restrict the authorizations for the normal users.

Figure 1 shows an overview of how the user authorizations are defined.

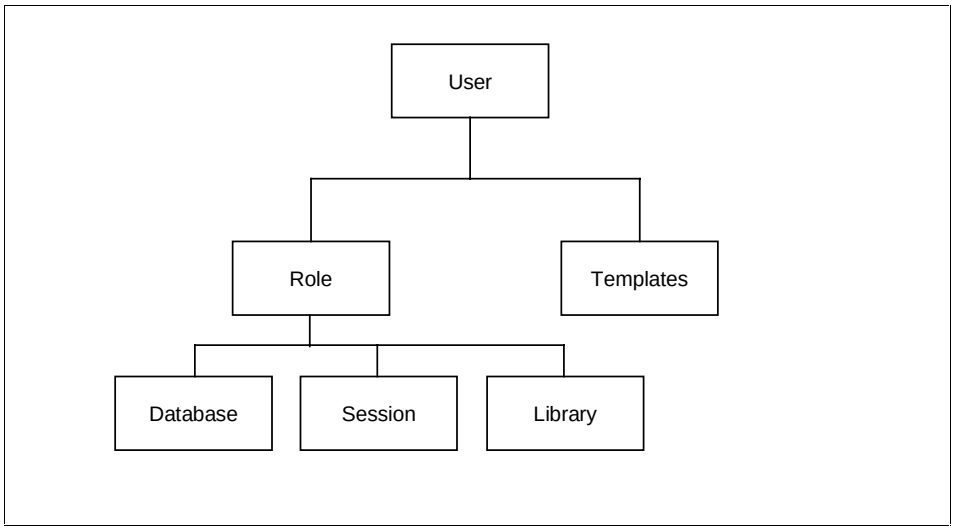


Figure 1. User authorizations based on roles and templates

The user's authorizations are defined in the role and some additional authorizations are defined in templates. These templates contain development parameters, device preferences, and so on.

The role-authorization procedure is described in chapter 3. The template authorizations are described in chapter 4.

Text Parameters

The Text Parameters business object is part of the Text Management module. Some of the parameters, such as the Text Group and Text Field authorizations, are used as input for the User Management module. These parameters are discussed in this module procedure where necessary.

Developers Data

The Developers Data business object is part of the Application Development (ADV) module. However, the parameters are also used as input for BaanERP users who are responsible for the development of customized software components. These parameters are discussed in this module procedure where necessary.

Miscellaneous

You can use the Miscellaneous business object to print or delete the user history. You can also use this business object to remove the default settings that have been defined by the user for other sessions.

1.3 The modules related to User Management

You can use the Database Administrator (DBA) module in Baan Tools to create database users. A database user is a BaanERP user who is authorized to access a database. The configuration information for the database user contains all necessary settings to logon to a database. These settings are automatically loaded when the BaanERP user logs on.

You can use the AMS business object, which is part of the User Management module, to restrict the BaanERP user's database authorizations.

2. Creating BaanERP users

This chapter describes how you can use the User Management module to create BaanERP users. Most of the steps in the procedure are part of the General User Data business object. Some additonal user parameters are set in other bussines objects.

The procedure's results

With this procedure, the user can start BaanERP and use the menu browser. The user can start sessions from the menu browser. The BaanERP user also has permissions on a database level that can be restricted with the AMS business object.

Figure 2 shows the steps in the procedure.

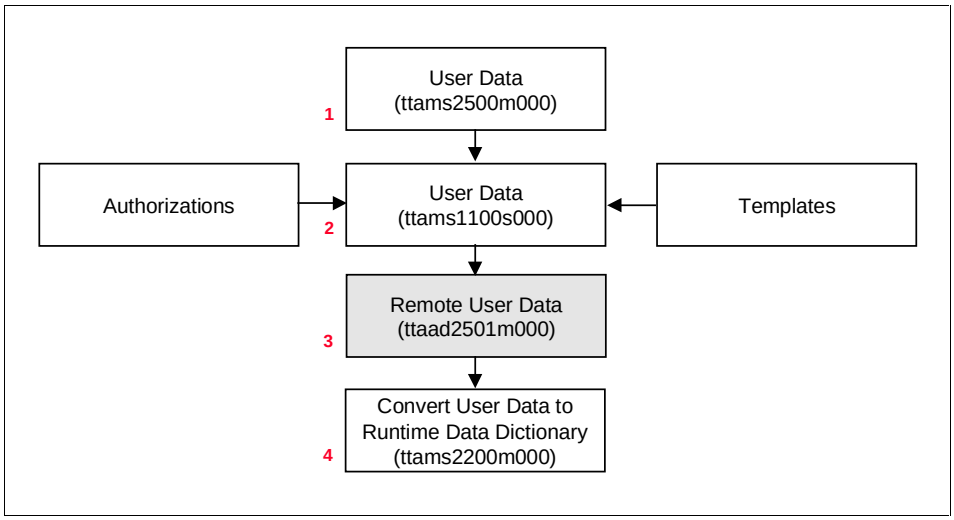


Figure 2. Creating the BaanERP user

The procedure that you can use to create BaanERP users consists of the following steps.

Step 1 User Data (ttaad2500m000)

You can use this session as the beginning and end of the procedure. Click **New** on the toolbar to start the details session. In the details session you can define the basic user data. The **Specific** menu supplies the tools to:

- Convert the user's data to run-time when the procedure is completed.
- Give the BaanERP user database permissions. For a detailed description refer to the Database Administrator module description (UP007A US).

Step 2 User Data (ttams1100s000)

You can use this session to define the basic user data for the BaanERP user. The basic data contains:

- The system data
- The defaults settings. For example, the roles and templates to which the user is linked
- The authorizations of the user

System Data

You can use this tab to define the name of the user, the user's BaanERP system logon, the user type, the package combination, the default company, the language code of the BaanERP software, and the startup data.

You can make a distinction between two user types:

- Normal users, which have restricted authorizations for starting sessions, accessing table fields, working with data pertaining to specific company numbers, and so on.
- Super users, which have unrestricted authorizations.

The restrictions on the authorizations are defined with the Authorization Management System (AMS).

The startup data consists of:

- The startup menu
- The startup program

The startup program defines how BaanERP is presented to the user after startup. You can select one of the following options:

- The **Menu Browser**, a graphical user interface between BaanERP and the users representing the menu structure.
- The **Desktop Manager**, a graphical user interface between BaanERP and the users that represent group icons and item icons. These group icons and item icons represent related items such as BaanERP programs and sessions. You must define a desktop name for this option.
- The **Dynamic Enterprise Modeler (DEM)** browser, which represents the BaanERP functionality in business processes.
- The **Workflow Client**, which represents the work items (tasks) of the users according to their role in the company.

Defaults

You can use this tab to define some general Windows settings and the templates that contain the common data relevant to the user.

If you select the **Save and restore Windows Defaults** check box, the position and size of a session's window is saved when you quit Windows. At the next startup, the window is displayed in the same position and size as when you last quit the session was last exited.

You can select one or more of the following templates:

- User Data
- Default Text Groups
- Default Text Fields
- Development Parameters
- Device Preferences

Refer to chapter 4 for a detailed description of the templates

Authorizations

The data on this tab is password protected and can only be changed by system administrators and users with system administrator permissions.

You can use this tab to define the role(s) of the user and the templates that define some of the general authorizations of the users.

If you select the **Auth for all Package VRCs** check box the developer can customize software components in all package VRCs. If you define a package VRC in the Developer Authorization template, this check box is overruled and the developer will no longer be authorized for all package VRCs. The developer will only be authorized for the package VRCs that are defined in the template.

The package VRCs that you define in the Developers Authorization template are also the package VRCs for which the developer is authorized if the **Auth for all Package VRCs** check box is cleared.

You can select one or more of the following authorization templates:

- Terminal authorizations, which define the terminals the user can use to start BaanERP.
- Developers authorizations, These define the package VRCs, languages and modules for which the developer is authorized to customize software components. This template also defines whether or not the developer is authorized to customize software components that are created by other developers.
- Text Group authorizations. These define the text groups for which the normal user must have **Use**, **Read**, or **Update** authorizations.

Step 3 Remote User Data (ttaad2501m000)

You can use this optional session if the BaanERP user must be able to work with distributed or remote databases, or split user interfaces. You can define the remote system and remote system logon. The remote user file is used to make the connection to the remote system for a specific user.

For example, the user must be able to start BaanERP from a workstation while the database is located at another system. To make this possible it is necessary that the remote user file must be created on the workstation.

Step 4 Convert User Data to Run-time Data Dictionary (ttams2200m000)

You can start this session from the **Specific** menu in the User Data (ttaad2500m000) session. You can use this session to convert the user file, or changes to the user file, to the run-time data dictionary. You must restart BaanERP to activate the changes.

2.1 Defining additional user settings

Some user parameters or default settings are defined in other business objecs then General User Data. For example:

- Developers Data
- Default Settings

Developers Data

Some of the user's parameters and templates are defined in the Developers Data business object. For example:

- The current package VRC
- The developer's authorization password
- The development parameters templates
- The developer authorizations template

Change Current Package VRC of User (ttadv0140m000)

The current package VRC is the package VRC for which the user is allowed to develop software components. You can use this session to specify or change the current package VRC for a user.

If you select the **Show Current VRC only (Multilevel)** check box, only the valid software components are shown in sessions that are used to develop software components. For example, the components with the latest VRC in the derivation structure of the current package VRC. Only the components of the current package VRC can be changed.

Change Password for Developer Authorizations (ttadv0143m000)

The Authorization tab in the User Data Details (ttams1100s000) session and the Developer Authorization Template (ttams1151m000) session are password protected. The system administrator uses this session to change the user's password. The password is also needed for the General Table Maintenance (ttaad4100) session.

Some development parameters and authorizations are defined in templates. Refer to chapter 4 for a detailed description of these templates.

Default Settings

You can use the Default Settings business object to customize the user environment in which users have their own startup sessions. You can specify the startup sessions in the session groups, and the run-time resources. The default settings are defined in the following sessions:

- Maintain Sessions Groups (ttaad2107m000)
- Maintain Startup Sessions (ttaad2106m000)
- Maintain User Settings (ttaad2105m000)
- Runtime Resources (ttdsk3160m000)

Maintain Session Groups (ttaad2107m000)

You can use this session to define a session group that will contain the user's startup sessions. Startup sessions are sessions that are activated automatically when BaanERP is started.

Maintain Startup Sessions (ttaad2106m000)

You can use this session to add the startup sessions to the session group.

Maintain User Settings (ttaad2105m000)

You can use this session to link a session group to a user.

Runtime Resources (ttdsk3160m000)

You can use this session to define BaanERP's run-time resources. The run-time resources include the colors and fonts used in the windows, and sizes and fonts for messages and questions.

2.2 The sessions that are related to the main procedure

The General User Data business object can also be used to change the package combination for a user or a range of users. This session is not dirctly used in the procedure to create a BaanERP user but it is a helpful user management tool.

Change Package Combinations for Users (ttaad2200m000)

You can run this session, for example, when you have changed the package combination of a company in the Change Package Combination by Company (ttaad1101m000) session.

This session can only change the user's package combination into one that matches the package combination of the user's default company. The company's package combination can only differ from the new user's package combination under the following conditions:

- Both package combinations include the same packages
- Different package VRCs are used in the package combinations

The package VRCs can only differ if:

- Both VRCs are derived from each other
- Both package VRCs are derived from the same VRC and no changes in data definitions or domains have been made in the derived VRCs

The Miscellaneous business object gives you the tools to:

- Print the user history
- Delete the user history
- Remove the users default settings

Print User History (ttaad2402m000)

You can use this session to print the history for a range of users. The user's history report can be sorted by user or date/time and contains the names of the users and the sessions they have used, with the start times and end times. The data is printed from a sequential file ($BSE/lib/TIME.HIS) and can therefore take a long time to print.

Note

The user's history is only logged if the **History** check box in the user's data template is selected.

Delete User History (ttaad2202m000)

You can use this session to delete the contents of the history file.

Remove the Users Default Settings (ttstpdeldeflt)

You can use this session to remove the user's defaults settings. A user can define default settings by session, to avoid having to re-enter regularly used parameters.

3. Defining the normal user's authorizations with the AMS business object

This chapter describes how you can use AMS:

- To define roles and subroles
- To define the authorization per role and subrole
- To convert the roles and authorizations to the run-time data dictionary

Note

The authorizations for normal users can be restricted, while the super users will retain unrestricted authorizations.

The AMS procedure's result

A user environment with clearly defined tasks and duties for all normal users, by authorizing the normal users according to their role in an organization.

For a BaanERP user to work with BaanERP, you must define their function and the related authorizations for their function in the AMS business object. The AMS procedure consists of the following steps:

1. Define the roles and subroles for an organization
2. Define the approperiate authorizations per role
3. Link the BaanERP user to a role
4. Convert the user data file to the run-time data dictionary

3.1 Defining user roles and subroles

AMS gives you the functionality to define the restricted authorizations for normal users based on their role in a company. The user's user data and the user's authorizations for BaanERP are defined in their role. You can define more than one role per user and more than one sub role per role. For example, a department manager has more responsibilities than the employees in a department. The manager has two roles:

- The role of the employee with the appropriate authorizations
- The manager's role with additional authorizations relevant only to the manager

Figure 3 shows the combined authorizations of two roles in one role. For example, if a user has permission for a database and another role states that the user has no permission for that database, the user will ultimately have permission.

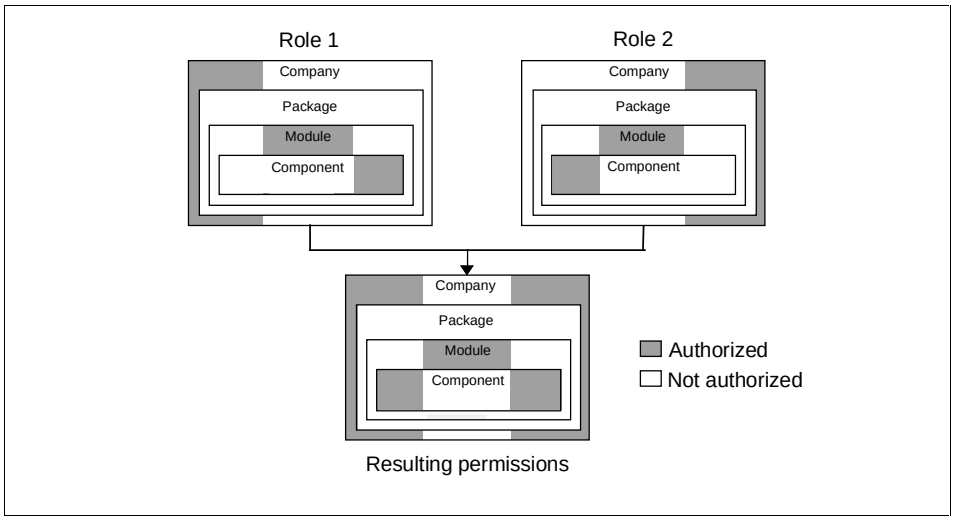


Figure 3. Determining the resulting permissions for a combination of roles

Role Data (ttams2100m000)

This session is the starting point for the AMS procedure. You can use this session to define the roles and subroles. From the **Specific** menu, you can start all sessions that you need to:

- Define subroles in a role
- Define the authorizations per role
- Convert the role data to the run-time data dictionary

From the **Specific** menu, you can also start the Rolebrowser that presents the roles and subroles in a graphical user interface. Refer to chapter 5 for a detailed description of the Rolebrowser.

3.2 Defining authorizations per role and subrole

If you define the authorizations by role instead of by user, you can reduce the redundant data significantly. It also provides a user-friendly method to add new users, or to update user authorizations.

Note

This procedure describes how you can define the user's role dependent authorizations. Refer to chapter 4 for a description of the authorization templates.

The role authorizations are defined for the following software components in BaanERP:

- Sessions
- Databases, divided into:
  - Tables
  - Table Fields
- Libraries

You can restrict the user's authorizations to a specific company, or define the authorizations for all companies. The authorizations defined for a specific company will have the highest priority.

You must define a time-interval, in which the user is authorized to start sessions. This is a helpful option that you can use, for example, to restrict users to start time consuming processes during the day. These processes can lead to a decrease in performance and to longer response times.

The authorizations can be defined at several levels. For example:

- At company level (not applicable for libraries)
- At package level
- At module level
- At component level. For example, sessions, database tables, and so on.
- At subcomponent level. This level is only applicable for database tables and refers to the database table fields

A conversion indicator is set as soon as there is a change in the authorization data. The conversion to run-time is only carried out when it is really necessary. You can also conduct a full conversion to the run-time data dictionary, independent of the conversion indicators. If the conversion is completed successfully, the conversion indicator for the role is cleared.

Note

The session authorizations and the library authorizations are handled in the same way. The session authorizations and library authorizations are stored in one file.

In the Role Data (ttams2100m000) session, you can click **Start the Sessions Needed** from the specific list to define the session authorizations, database authorizations, and the library authorizations at the appropriate levels.

Session authorizations

AMS gives you the tools to print, display, maintain, and convert the session authorizations for a group of users who are identified by a role in an organization.

Table 1 shows an overview of the session authorizations priority.

	Specific company	All companies
Session authorization per session	1	2
Session by authorization per module	3	4
Session authorization per package	5	6
Session authorization per company	7	8

Table 1. Priority of session authorization checks

The table shows that the session authorization with the highest priority (1) is stated at the most specific level and the lowest priority (8) is stated at the most global level.

You can define the session authorizations with the following sessions:

- Session Authorizations by Company (ttams3133m000)
- Session Authorizations by Package (ttams3130m000)
- Session Authorizations by Module (ttams3131m000)
- Session Authorizations by Session (ttams3132m000)

In all these sessions, you must do the following:

- Select the **All Companies** check box to define the session authorizations for all companies, or specify a specific company in the **Company** field. The session authorizations that you define for a specific company will have a higher priority than those defined for all companies.
- Define the actions that are permitted for the sessions in the **Authorizations Groups** field. For example, full authorization, no authorization, display, insert, delete, modify, and so on. BaanERP uses this information to determine what a normal user can do in the session.
- Define in the **Start Time** and **End Time** fields the time interval in which the normal users are authorized to activate a session.

In the sessions normal users are autorized to activate, you can use the **Specific** menu to start the sessions needed to:

- Change the defined time interval
- Copy a range of companies, packages, modules, or sessions in the current role
- Convert the changes of the session authorizations to the run-time data dictionary

Session Authorizations by Company (ttams3133m000)

You can use this session to define the session authorizations at company level, per role. This means that you can give the normal users who are linked to the role, restricted access to data for a specified range of companies.

You can create exceptions to the session authorizations at company level per role at the following levels:

- At package level with the Session Authorizations by Package (ttams3130m000) session
- At module level with the Session Authorizations by Module (ttams3131m000) session
- At session level with the Session Authorizations by Session (ttams3132m000) session

Session Authorizations by Package (ttams3130m000)

You can use this session to define the session authorizations, at package level, per role. This means that the normal user that is linked to the role can be restricted to a specified range of packages in a company.

The session authorizations at package level are an exception to the session authorizations at company level. You can define exceptions to the session authorizations at package level per role at the following levels:

- At module level with the Session Authorizations by Module (ttams3131m000) session
- At session level with the Session Authorizations by Session (ttams3132m000) session

Session Authorizations by Module (ttams3131m000)

You can use this session to define the session authorizations at module level, per role. This means that the normal user can be restricted to a specified range of modules in a package.

The session authorizations at module level are an exception to the session authorizations at company level, and an exception to the session authorizations at package level.

You can define exceptions to the session authorizations at module level per role and at session level with the Session Authorizations by Session (ttams3132m000) session.

Session Authorizations by Session (ttams3132m000)

You can use this session to define the session authorizations at session level per role. This means that the normal user can be restricted to a specified range of sessions in the module.

The session authorizations at session level are an exception to the session authorizations at the following levels:

- At company level
- At package level
- At module level

Database authorizations

AMS gives you the tools to print, display, maintain and convert the database authorizations for a group of normal users who are identified by a role. The database authorizations are divided into:

- Database table authorizations
- Database table field authorizations

You can define the database authorizations on several levels. Table 2 shows an overview of the database authorizations priority.

	Specific company	All companies
Database table per table data	1	2
Database table per table	3	4
Database table per module	5	6
Database table per package	7	8
Database table per company	9	10

Table 2: Priority of table authorization checks

The table shows that the database authorization with the highest priority (1) is stated at the most specific level and the lowest priority (10) is stated at the most global level.

You can define the database table authorizations and the database table field authorizations with the following sessions:

- Table Authorizations by Company (ttam3144m000)
- Table Authorizations by Package (ttam3140m000)
- Table Authorizations by Module (ttam3141m000)
- Table Authorizations by Table (ttam3142m000)
- Table Data Authorizations (ttam3145m000)
- Table Field Authorizations (ttam3143m000)
- Table Field Data Authorizations (ttam3146m000)

In all of these sessions you must do the following:

- Select the **All Companies** check box to define the database authorizations for all companies, or specify a specific company in the **Company field**. The database authorizations that you define for a specific company will have a higher priority than those defined for all companies.
- Define in the **Authorization Indicator** field the database actions that are allowed for the normal users who are linked to the role. For example, Delete/Insert/Modify/Read, Insert/Modify/Read, Modify/Read, Read or Not Authorized. The database server uses this information to determine what a user is allowed to do in the database.

In these sessions, you can use the **Specific** menu to start the sessions needed to:

- Modify database authorizations
- Delete database authorizations
- Copy a range of companies, packages, modules, or tables from the data dictionary in the current role
- Convert the changes of the database table authorizations to the run-time data dictionary

Table Authorizations by Company (ttam3144m000)

You can use this session to define the database table authorizations at company level, per role. This means that the normal users who are linked to the role can be restricted to specific actions on records in database tables for a specified range of companies.

You can define exceptions to the table authorizations at company level at the following levels:

- At package level with the Table Authorizations by Package (ttam3140m000) session
- At module level with the Table Authorizations by Module (ttam3141m000) session
- At table level with the Table Authorizations by Table (ttam3142m000) session
- At table data level with the Table Data Authorizations (ttam3145m000) session

Table Authorizations by Package (ttam3140m000)

You can use this session to define the database table authorizations at package level, per role. This means that the normal users who are linked to the role can be restricted to specific actions on records in database tables, for a specified range of packages in a company.

The database table authorizations at package level are an exception in the database table authorizations session at company level. You can define exceptions to the database table authorizations at package level at the following levels:

- At module level with the Table Authorizations by Module (ttam3141m000) session
- At table level with the Table Authorizations by Table (ttam3142m000) session
- At table-data level with the Table Data Authorizations (ttam3145m000) session

For example, a normal user who is linked to the role has authorization to insert, to modify, or to read data in Baan Distribution. The user has no authorization over the Sales Order Data module.

Table Authorizations by Module (ttam3141m000)

You can use session to define the database table authorizations at module level, per role. This means that the users who are linked to the role can be restricted to specific actions on records in database tables for a specified range of modules in a package.

The database table authorizations at module level are an exception to the database table authorizations at company level and at package level.

You can define exceptions to the database table authorizations at module level at the following levels:

- At table level with the Table Authorizations by Table (ttam3142m000) session
- At table-data level with the Table Data Authorizations (ttam3145m000) session

Table Authorizations by Table (ttam3142m000)

You can use this session to define the database table authorizations at table level, per role. This means that the users who are linked to the role can be restricted to specific actions on records in database tables for a specified range of tables in a module.

The database table authorizations at table level are an exception to the database table authorizations at company level, at package level, and at module level.

You can define exceptions to the database table authorizations at table-data level with the Table Data Authorizations (ttam3145m000) session.

Table Data Authorizations (ttam3145m000)

You can use this session to define table data authorizations, per role. This is the most specific database table authorization that you can define. This means that you can define restrictions for normal users who are linked to the role.

You can define table data authorizations for data in a table with a condition.

The authorization that is defined in this session can be an exception or addition to the table authorizations at all levels. You can use table data authorizations to block specific data in the database for normal users who are linked to the role. You can define authorizations depending on the data of a table. For example, a user can only be allowed to insert sales orders when the order number is between 100.000 and 200.000.

You can specify an authorization level for each condition. For example, the data authorization. This can be another authorization level as the table authorization level, which is defined in the database table authorization sessions. If you have not specified table authorizations, the table authorization status is delete, insert, modify, or read.

An overlap can occur between two conditions for the same table with different authorization levels. In that case, the most restrictive authorization level is overruling.

The table data authorizations are an exception to the database table authorizations at the following levels:

- At company level
- At package level
- At module level
- At table level

Table Field Authorizations (ttam3143m000)

You can use this session to define database table authorizations at table field level. This means that you can restrict the normal users who are linked to the role to fields of a specific table in a module.

Note

Database table-field authorizations are only meaningful if the user has at least Read authorization for the database table. The database table-field authorizations are only functional for sessions with a main table. For example, maintain sessions and display sessions.

If a user has no authorization to modify a field, the field is disabled. If a user has no authorizations at all, the **No Authorization Character**, which is defined in the Character Parameters (ttaad0100m000) session, is displayed. Database table field authorizations have no effect on reports. Update sessions, when fields are automatically filled by the session, will also ignore database table-field authorizations.

If you do not specify database table-field authorizations, the user will have the database table authorizations.

You can define exceptions to the database table-field authorizations at table-field data level in the Table Field Data Authorizations (ttam3146m000) sessions.

Table Field Data Authorizations (ttam3146m000)

You can use this session to define table field data authorizations. This is the most specific database table field authorization that you can define. It means that you can define restrictions for normal users who are linked to the role, to database actions on fields of a table for a given condition.

Table field data authorizations are specified in a table, for a range of data by defining a condition. The authorization, which is defined in this session can be an exception or an addition to the authorizations that are defined in the Table Field Authorizations (ttam3143m000) session.

You can define authorizations depending on the data of a table field. For example, a user can be allowed to view the order price when the order number is between 100.000 and 200.000.

You can specify an authorization level for each condition. For example, the read/write authorization. This can be authorization level other than the table authorization level, which is defined in the database table field authorization sessions. If you have not specified table field data authorizations, the table authorization is the same as the database table authorization of the table.

An overlap can occur between two conditions for the same table with different authorization levels. In such a case, the most restrictive authorization level is taken in.

Library authorizations

BaanERP uses OLE, DDE, OCX and ORB interfaces to integrate programs with the BaanERP environment. These programs communicate with BaanERP through the Dynamic Link Libraries (DLLs). AMS gives you the tools to print, display, maintain and convert the Dynamic Link Library authorizations for a group of users who are identified by a role.

You can define library authorization types for the library authorizations. BaanERP uses this information to determine whether a user is authorized to use the functions in a library.

The library authorizations can be specified on several levels. Table 3 shows an overview of the library authorizations priority.

Library per library	1
Library per module	2
Library per package	3

Table 3. Priority of library authorization checks

The table shows that the library authorization with the highest priority (1) is stated at the most specific level and the lowest priority (3) is stated at the most global level.

You can define the library authorizations with the following sessions:

- Library Authorizations by Package (ttams3150m000)
- Library Authorizations by Module (ttams3151m000)
- Library Authorizations by Library (ttams3152m000)

You can use the **Specific** menu in these sessions to start the sessions needed to:

- Copy a range of packages, modules, or libraries in the current role
- Convert the changes of the library authorizations to the run-time data dictionary

Library Authorizations by Package (ttams3150m000)

You can use this session to define the library authorizations at package level, per role. This means that you can authorize or deny the authorization of normal users who are linked to the role, to use the library functions for a specified range of packages.

You can create exceptions on the library authorizations at package level at the following levels:

- At module level with the Library Authorizations by Module (ttams3151m000) session
- At library level with the Library Authorizations by Library (ttams3152m000) session

Library Authorizations by Module (ttams3151m000)

You can use this session to define the library authorizations at module level, per role. This means that you can authorize, or deny the authorization of normal users who are linked to the role, to use the library functions for a specified range of modules in a package.

The library authorizations at module level, for each role, are an exception to the library authorizations at package level. You can create exceptions to the library authorizations at the module level, and at library level with the Library Authorizations by Library (ttams3152m000) session.

Library Authorizations by Library (ttams3152m000)

You can use this session to define the library authorizations at library level, per role. This means that you can authorize or deny the authorization of normal users who are linked to the role, to use the library functions for a specified range of libraries ina package.

The library authorizations at library level, for each role, are an exception to the library authorizations at module level, and at package level.

3.3 Connecting the BaanERP user to a role

The next step in the AMS procedure is to link the BaanERP user to a role. The BaanERP user is created with the User Data (ttaad2500m000) session. Return to this session. Select and double-click the user's logon to start the User Data (ttams1100s000) details session. On the **Authorizations** tab, you can enter the user's roles.

Note

The data on the **Authorization** tab is password protected, and can only be edited by system administrators or users with system administrators authorizations.

3.4 Convert the user file to the runtime datadictionary

To complete the AMS procedure, you must convert the user data file and role data file to the runtime data dictionary. Go to the User Data (ttaad2500m000) session and select the user's logon. On the **Specific** menu, choose **Convert to Runtime DD** to start the Convert to Runtime DD (ttams2200m000) session.

Convert to Run-time DD (ttams2200m000)

You can use this session to convert the changed user data and role data for a user, or a range of users, to the run-time data dictionary. To make the changes to the user data and role data effective, you must restart BaanERP.

The following user related data is dumped in the ${BSE}/lib/user/<user> file:

- User data
- Data in the user data template
- Language dependent data
- Company dependent data
- Default users settings
- Data in the terminal authorization template

The role related data is divided over the following authorizations:

- The session authorizations and library authorizations are dumped in the ${BSE}/lib/roles/session/<first char>/<role>/ file.
- Database authorizations are dumped in the ${BSE}/lib/roles/db/<first char>/<role>/ file.

4. Using templates in AMS

This chapter describes how you can use AMS:

- To define templates that contain data for a group of users
- To convert the templates to the run-time data dictionary
- To connect the BaanERP user to a template

Note

The templates define the user related data and authorizations on a user level, not on a role level. If you define the user related data in a template and then link a group of users to that template, you can reduce the redundant data significantly. It also provides a user-friendly method to change the data in the templates.

The user's authorizations are ultimately a combination of the authorizations that are defined in the templates and roles, connected to the user profile. The templates are linked to a user in the User Data (ttams1100s000) details session.

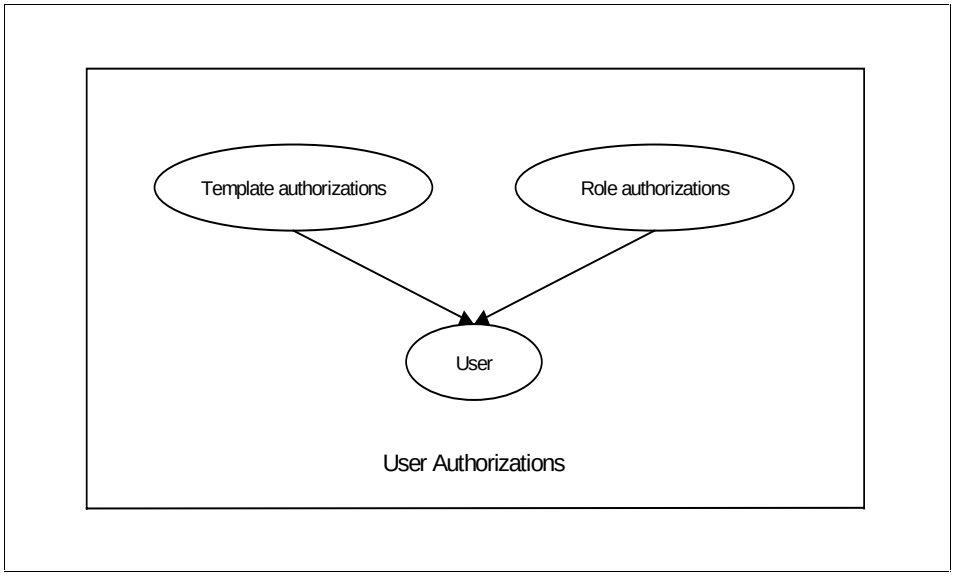


Figure 4. Schematic overview of the user authorizations

4.1 Defining Templates that contain data for a group of users

You can use AMS to create templates to define the common user data and additional parameters, which are required by users who will customize software components. The data is defined in templates with the following sessions:

- User Data Template (ttams1110m000)
- Development Parameters Template (ttams1150m000)
- Developer Authorization Template (ttams1151m000)
- Text Group Authorization Template (ttams1122m000)
- Default Text Groups Template (ttams1121m000)
- Default Text Groups by Text Field Template (ttams1120m000)
- Device Preference Template (ttams1140m000)
- Terminal Authorization Template (ttams1130m000)

User Data Template (ttams1100s000)

You can use this session to define default settings and parameters, for a group of BaanERP users, in a template. The default data contains the system data and the authorization data. The system data defines, for example :

- The application server, for example b-shell
- The system from which the users start the application
- The online Help format, for example Windows Help or HTML Help
- The time between the printout and deleting the temporary file
- The Triton Super Set characters
- The refresh interval
- If a history log can be created of the user's actions
- If the session code must be shown in the title
- If the UI Page mode must be activated

The authorization data defines, for example:

- The time interval defined by a start time and an end time
- The shell command type
- The shell command
- If the session must be called by the session code
- If a session can be started from the helpviewer
- If the users are authorized for all devices
- The time zone

Development Parameters Template (ttams1150m000)

Some parameters that are used by application developers are defined in a template. For example, you can choose to run an automatic compilation after you have created/changed menus or forms. You can also specify commands and options which the user can employ in the development environment.

The template is linked to a user with the proper development authorizations in the User Data details (ttams1100s000) session on the **Defaults** tab.

Application parameters are settings that are needed by the application developer to develop software components. There are parameters available for:

- Automatic compilation to the Run-time Data Dictionary after changing forms or menus
- Actions after the option <Copy to current package VRC>
- The parameters that the editor can use to develop software

Developer Authorization Template (ttams1151m000)

Some of the developer's authorizations are defined in a template. The template is linked to a user with the proper development authorizations in the User Data details (ttams1100s000) session on the **Defaults** tab.

In the template you can specify:

- The package VRC for which the developer is authorized to maintain and develop software components.
- The languages and modules of the specified package VRC for which the developers are authorized to maintain and develop software components.
- The status up to which the technical writer is authorized to maintain the Help texts.

If you select the **All Modules** and **All Languages** check boxes, the users who are linked to the template are authorized to maintain and develop software components in all modules in BaanERP, and in all languages. If the check boxes are cleared, you must specify the modules and languages for which the user must be authorized.

If you select the **Authorization for Component of other Developer** check box, the user is authorized to maintain the software components that are created by other users during their absence. This is a helpful option, for example, for a senior application developer.

Text is used in BaanERP for several different purposes. For example, for online Help, to provide information on the data stored in the database tables, or to use the text editor to write queries. A normal user must have some basic authorizations to use, update, or read text. The necessary data and authorizations are defined in the text parameters. The text parameters are part of the Text Management module. Some of the text parameters are defined in templates in the User Management module. The user's text parameters are defined in templates with the following sessions:

- Text Group Authorization Template (ttams1122m000)
- Default Text Groups Template (ttams1121m000)
- Default Text Groups by Text Field Template (ttams1120m000)

The text parameters can be specified for a specific company or for all companies. If you select the **All Companies** check box in these sessions, the users who are linked to the templates are authorized to edit text in all companies. If you want to restrict the users to a specific company, you must define that company in the **Comp** field. The text parameters that are defined for a specific company take precedence over defaults that are defined for all companies.

Text Group Authorization Template (ttams1122m000)

You can use this session to define the use, update, or read authorizations for normal users per text group in a template. A text group is a means to define how text must be presented in a window by defining the text editor, default window, and dimensions of the window. Refer to the Text Management Module for more details.

Default Text Groups Template (ttams1121m000)

You can use this session to define default text groups in a template. If a text is written in a text field for which no default text group is defined, BaanERP will use the default text group that is defined in this template.

Default Text Groups by Text Field Template (ttams1120m000)

You can use this session to define default text groups for text fields in BaanERP, in a template. If a text is written in a text table field, it is linked to the default text group of that field

You must define the devices that can be used by the users, and the terminals from which the users can start BaanERP, in templates with the following sessions:

- Device Preference Template (ttams1140m000)
- Terminal Authorization Template (ttams1130m000)

Device Preference Template (ttams1140m000)

You can use this session to define devices and an order of preferences in a template.

Note

If the template is linked to a user who is not authorized for all devices, the user is only authorized to use the devices that are defined in the template. You can authorize a user for all devices. To do this, select the **Authorization for all devices** check box in the user data template.

Terminal Authorization Template (ttams1130m000)

You can use this session to define a number of terminals in a template. This template can only be used if the terminals are connected to fixed tty ports.

In the template enter the code of the tty ports to which the terminals are connected. Or, from the **Specific** menu, choose **Import Terminals** to view a range of terminals. Delete the terminals from the range, that you do not want to define in the template.

4.2 Convert the templates to the run-time data dictionary

Changes to the template can be converted to the run-time data dictionary, per template. From the **Specific** menu in these sessions, choose **Convert to Runtime DD** to start the Convert to Run-time DD (ttams2200m000) session. Refer to 3.4 for a detailed description of this session.

4.3 Connecting the BaanERP user to a template

The BaanERP user is created with the User Data (ttaad2500m000) session. Return to this session. Select and double-click the user's logon to start the User Data (ttams1100s000) details session. On the **Authorizations** tab, you can enter the templates for the user.

Note

The data on the **Authorization** tab is password protected, and can only be edited by system administrators or users with system administrators authorizations.

5. Using the Role Browser

You can use the Role Browser in a browser to view (part of) the role tree. The role tree represents a role with all its subroles, that can also contain sub roles.

In the Role Browse, double-click a role folder to display the sub roles in the role. Select a role, or subrole, and choose **Start AMS** on the **Options** menu to start the Role Data (ttams2100m000) sessions. The role browser highlights cyclical definitions in the tree. These cyclical role definitions are not allowed and have to be removed.

The role browser uses the display logic of the existing desktop browser, to ensure a consistent interface over the various browsers in BaanERP.

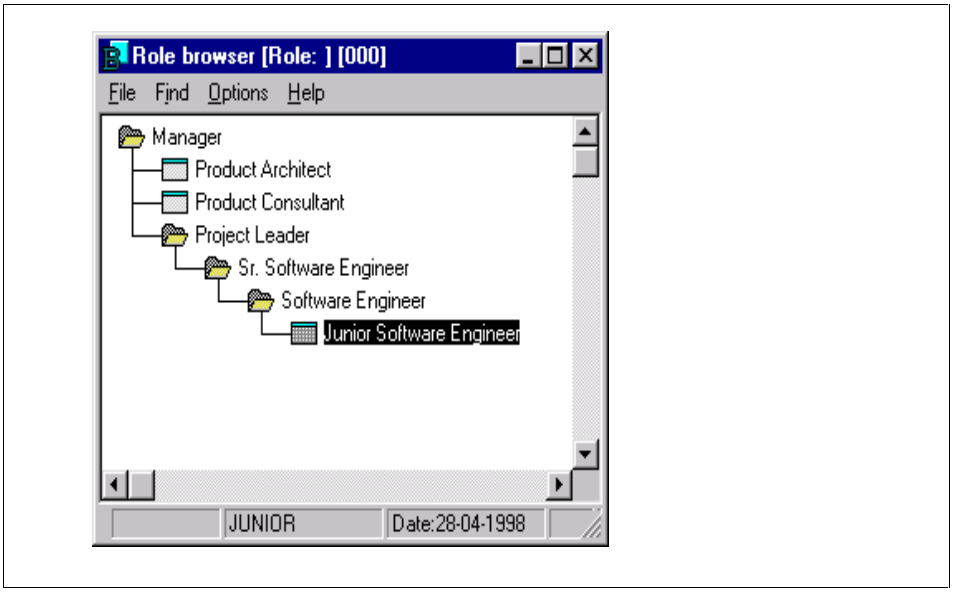


Figure 5. The role browser

Figure 5 shows an example of roles with subroles. The manager has a number of roles linked to the manager role. The managers does not only have the manager's authorizations, but also the authorizations of the product architect, product consultant, and project leader, which are defined in their respective roles. The project leader role has additional subroles. The role browser shows all the manager's authorizations, from his own role to the role of the lowest ranked employee.

Figure 6 shows an example of a cyclical role. The Junior Software Engineer has also the role of the Senior Software Engineer, which of course is not the case.

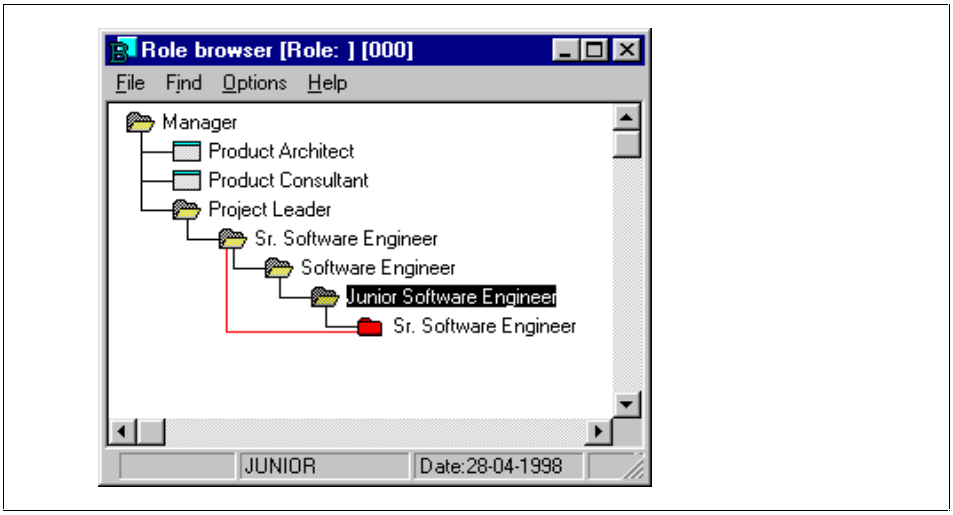


Figure 6. A cyclical role